Abstract

This specification defines the stream format and initialization data for using ISO Base media File Format [BMFF] content using the ISO Common Encryption ('cenc') protection scheme [CENC-1ST] and ISO MPEG-2 TS [MPEG2TS] using the ISO Common Encryption (‘cenc’) protection scheme [CENC-MPEG2TS] with the Encrypted Media Extensions. It also defines a common SystemID and PSSH box format for use with Encrypted Media Extensions.

1. Stream Format

Under the ISO Common Encryption ('cenc') protection scheme [CENC-1ST], ISO Base media File Format [BMFF] content is encrypted at the sample level with AES-128 CTR encryption. This protection method enables multiple Key Systems to decrypt the same media content.

Each key is identified by a Key ID and each encrypted sample is associated with the Key ID of the key needed to decrypt it. This association is signaled either through the specification of a default Key ID in the track encryption box ('tenc') or by assigning the sample to a Sample Group, the definition of which specifies a Key ID. Common encryption files may contain a mixture of encrypted and unencrypted samples.

ISO BMFF content encrypted using [CENC-1ST] can be directly translated without re-encryption to MPEG-2 TS [CENC-MPEG2TS]. In this case, a “CETS ECM” specified a Key ID.

2. Detecting Encryption

Protection scheme signaling conforms with ISO Base media File Format [BMFF]. When protection has been applied, the stream type will be transformed to 'encv' for video or 'enca' for audio, with a Protection Scheme Information Box ('sinf') added to the sample entry in the Sample Description Box ('stsd'). The Protection Scheme Information Box ('sinf') will contain a Scheme Type Box ('schm') with a scheme_type field set to a value of 'cenc' (Common Encryption).

The "encrypted block" is a sample. Determining whether a sample is encrypted depends on the corresponding Track Encryption Box ('tenc') and the sample group with grouping type 'seig' (CencSampleEncryption group), if any, associated with the sample. The default encryption state of a sample is defined by the IsEncrypted flag in the associated track encryption box ('tenc'). This default state may be modified by the IsEncrypted flag in the SampleGroupDescriptionBox ('sgpd'), pointed to by an index in the SampleToGroupBox ('sbgp').

Samples can be partially encrypted, specified by subsample information referenced by SampleAuxiliaryInformationSizesBox ('saiz') and SampleAuxiliaryInformationOffsetsBox ('saio') boxes.

For complete information, see [CENC-1ST].

The MPEG-2 TS ‘transport_scrambling_control’ field identifies the use of encryption when protected content in ISO BMFF is re-encapsulated in MPEG-2 TS [CENC-MPEG2TS].

3. Initialization Data and Events

Common Encryption files may contain one or more protection system specific header ('pssh') boxes, each for a unique SystemID at each location where a 'pssh' box is necessary.

A “CETS PSSH” packet [CENC-MPEG2TS] carries the complete payload of a `pssh` box when ISO BMFF protected content is re-encapsulated in MPEG-2 TS.

[CENC-MPEG2TS] **ISO/IEC 23001-9:2014** Information technology -- MPEG systems technologies -- Part 9: Common encryption of MPEG-2 transport streams

[MPEG2TS] **ISO/IEC 13818-1:2013** Information technology -- Generic coding of moving pictures and associated audio information -- Part 1: Systems